## REMARKS/ARGUMENTS

### Status of the Claims

Claims 1, 4-23, 34-36 and 38-43 remain in the application. New claims 44 to 53 have been added.

### Claim Amendments

Independent claim 1 has been amended to recite in part:

> " wherein delivering the plurality of decryption keys comprises:
>
> delivering to the customer processing platform a current key of the plurality of decryption keys;
>
> delivering to the customer processing platform a next key of the plurality of decryption keys; and
>
> causing the current key to be destroyed at the customer processing platform only after at least the next key of the plurality of decryption keys has been received."

Independent claims 16, 34, 35, 38 and 40 have been amended in a manner similar to that of claim 1.

Claims 2, 3 and 37 have been cancelled in addition to previously cancelled claims 24 to 33.

Dependent claims 4 and 5 have been made dependent on claim 1.

Dependent claims 6, 14, 20 and 39 have been amended to recite a feature wherein the plurality of sections of encrypted data content are downloaded via a peer-to-peer network and the plurality of decryption keys corresponding to the plurality of sections of encrypted data content are delivered over an encrypted decryption key delivery channel.

Dependent claim 16 has been amended to recite "destroying the decryption key only after completing playback of the encrypted section and beginning playback of the next encrypted section".

## 35 U.S.C § 103 Claim Rejections

In paragraph 3 of the Office Action, the Examiner rejects claims 1, 7-10, 13, 15, 35-38 and 40-42 under 35 U.S.C. 103(a) as being unpatentable over Peterka et al. (U.S. Patent Application Publication No. 2002/0170053 A1) in view of Feig et al. (U.S. Patent No. 7,251,833 B2);

In paragraph 4 of the Office Action, the Examiner rejects claims 2-6, 34 and 39 under 35 U.S.C. 103(a) as being unpatentable over Peterka et al. in view of Feig et al. and further in view of Giroux et al. (U.S. Patent Application Publication No. 2002/0078361 A1);

In paragraph 5 of the Office Action, the Examiner rejects claims 11 and 12 under 35 U.S.C. 103(a) as being unpatentable over Peterka et al. in view of Feig et al. and further in view of Granger et al. (U.S. Patent No. 6,334,189 B1);

In paragraph 6 of the Office Action, the Examiner rejects claims 14 and 43 under 35 U.S.C. 103(a) as being unpatentable over Peterka et al. in view of Feig et al. and further in view of Ginter et al. (U.S. Patent Application Publication No. 2006/0218651 A1);

In paragraph 7 of the Office Action, the Examiner rejects claims 16-18 and 21 under 35 U.S.C. 103(a) as being unpatentable over Feig et al. in view of Giroux et al.;

In paragraph 8 of the Office Action, the Examiner rejects claim 19 under 35 U.S.C. 103(a) as being unpatentable over Feig et al. in view of Giroux et al. and further in view of Granger et al.;

In paragraph 9 of the Office Action, the Examiner rejects claims 22 and 23 under 35 U.S.C. 103(a) as being unpatentable over Feig et al. in view of Giroux et al. and further in view of Watanabe et al. (U.S. Patent No. 7,114,073 B2); and

In paragraph 10 of the Office Action, the Examiner rejects claim 20 under 35 U.S.C. 103(a) as being unpatentable over Feig et al. in view of Giroux et al. and further in view of Ginter et al.

Applicant respectfully traverses the foregoing rejections for reasons stated below.

The law on obviousness under 35 U.S.C. 103 was recently addressed in ***KSR Int'l v. Teleflex, Inc.**, No. 04-1350, slip op. at 14 (U.S., Apr. 30, 2007).* Following this, examination guidelines were released on October 10, 2007 in regards to determining obviousness under 35 U.S.C. 103. According to these guidelines, the framework for the objective analysis for determining obviousness under 35 U.S.C. 103 is stated in ***Graham v. John Deere Co.** 383 U.S. 1,148 USPQ 459 (1966).* Obviousness is a question of law based on underlying factual inquiries. The factual inquiries enunciated by the Court are as follows:

(1) Determining the scope and content of the prior art;

(2) Ascertaining the differences between the claimed invention and the prior art; and

(3) Resolving the level of ordinary skill in the pertinent art.

The Graham factors, including secondary considerations when present, are the controlling inquiries in any obviousness analysis. Once the findings of fact are articulated, Office personnel must provide an explanation to support an obviousness rejection under 35 U.S.C. 103.

Applicant's analysis below demonstrates that the amended claims should be found novel and inventive, as an analysis following the factual inquiries laid out in Graham v. John Deere Co. clearly reveals the novel and inventive aspects of the claimed invention.

*Determining The Scope Of The Prior Art*

**Peterka et al.**

Peterka et al. describes a method for distributing encrypted data content which uses a hierarchy of encryption keys to provide for flexible billing options. Specifically, Peterka et al. describes a Pay-By-Time (PBT) billing option (See [0048]) in which a program is segmented into a plurality of program segments. The actual data of each respective program segment is then encrypted with at least one respective content key (CK). The respective content keys are then each encrypted with a respective program segment key (PSK). When a consumer wishes to join a multicast of the program, the consumer contacts an Origin Content Server (OCS) to begin receiving PSKs. The PSKs are distributed to the consumer in a multicast in which the PSKs are encrypted with the consumer's unique key (UK).

In order to actually view a program segment, the consumer must first decrypt the PSK corresponding to that program segment with the consumer's UK, then use that decrypted PSK to decrypt the CK corresponding to that program segment and then finally decrypt that program segment with the decrypted CK. In the Pay-By-Time billing method, the consumer must continue to request each new PSK in order to continue viewing the program, i.e. to continue decrypting program segments. Peterka also teaches that the content key for a future program segment may be encrypted with not only the PSK corresponding to the future program segment, but also with an old PSK of an old program segment. "Thus, if a user has not yet received a new program segment key, the content key can be obtained by utilizing the old program segment key." (see [0109] and Figure 9). Furthermore, Peterka et al. teaches that the content keys are maintained by the consumers, for possible use in later decryption. For example, Peterka describes a signalling method in which "a predetermined bit can be used to indicate if an **old or current content key should be used as opposed to a new content key** which has recently been distributed to the client." (see [0119]; emphasis added)

At the bottom of page 3 of the Office Action, the Examiner acknowledges that Peterka et al. fails to disclose "delivering to the customer processing platform a plurality of decryption keys corresponding to the plurality of encryption keys, wherein the decryption keys are delivered in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time."

In support of the rejection of unamended claims 1, 15 and 38, the Examiner has pointed to portions of Peterka et al. that teach "two PSK are distributed at a given time" and "that a client has possession of program segment key and the next key ... as well as content key 0, 1, 2, 3, 4, ...". However, as acknowledged by the Examiner, these portions of Peterka et al., which the Examiner asserts teach that the "client has possession of program segment key and the next key", merely teach that a current program segment key and a subsequent program segment key are made available to the client at any one given time.

**Feig et al.**

Feig et al. describes a method for enforcing the sequential playback of a multimedia file by partitioning the media file into a plurality of sequential data blocks, encoding each respective one of the sequential data blocks with a corresponding one of a plurality of encryption keys, transferring the encoded sequential data blocks to a receiving client, and streaming a plurality of decryption keys to the receiving client.

Feig et al. teaches that the decryption keys are streamed one at a time to the client to enforce sequential playback of the media file, but fails to describe any mechanism for preventing the client from retaining all of the decryption keys and all of the decrypted content once all of the decryption keys have been delivered to the client.

The Examiner has pointed to Figure 3 (steps 308-314), column 2, lines 40-65 and column 3 lines 1-5 of Feig et al. in support of the allegation that Feig et al. discloses "delivering to the customer processing platform a plurality of decryption keys corresponding to the plurality of encryption keys, wherein the decryption keys are delivered in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time". However, by the Examiner's own admission, these portions of Feig et al., and Feig et al. as a whole, merely teach that:

> "it is preferred that the token keys are transmitted to the client receiver by sequentially streaming each of the token keys, one at a time, enabling a one-to-one decryption and playback of the encrypted sequential data blocks"; and
>
> "[the] preferred method further includes sequentially decrypting each of the respective plurality of encrypted sequential data blocks using corresponding one of the plurality of cryptographic token keys ... and for playing back each recovered sequential data".

Applicant respectfully submits that the Examiner's own statements clearly demonstrate that Feig et al. merely discloses the sequential streaming of token keys to a client receiver and the decryption of encrypted content using the streamed token keys. There is no suggestion whatsoever in Feig et al. that each decryption key is delivered and then deleted or destroyed after decryption of the corresponding encrypted content segment in a manner that would prevent the client from simultaneously having possession of all of the decryption keys. In fact, Feig et al. clearly states that token keys (decryption keys) are retained by the customers once they are delivered. For example, column 2, lines 56 to 58 states that "all of the cryptographic token keys may also be transmitted to the client receiver as a single block of data for storage and later use" (emphasis added).

**Giroux et al.**

Giroux et al. teaches an information security architecture for encrypting and distributing a segment of electronic information for remote access while maintaining access control to the encrypted electronic information by dispensing decryption keys for the encrypted electronic information via a remote server 106 to an authorized user 116, and causing the user's decryption tool (viewing tool 104) to delete/destroy the decryption key after the encrypted segment of electronic information is decrypted. The decrypted electronic information is also destroyed once it is displayed on the viewing tool 104. It is important to note that Giroux et al. teaches that a next decryption key for a next encrypted segment of electronic information is not delivered to a customer until customer requests the next decryption key after the decryption of the current encrypted segment is completed, the decrypted information is displayed and the current decryption key has been deleted. See paragraph [0051], which states:

> "If the user 216 is authorized to access the section, the server 206 sends the decryption key and options for that section to the Application Utility 230 at the viewing user's computer 224 and the Application Utility 230 decrypts the section using the decryption key. After decrypting the section, the Application Utility 230 immediately discards/destroys the key, loads the decrypted section into the display buffers to render the decrypted section to the screen, and then clears the buffers to destroy the decrypted version of the section. When the viewing user moves to a different section, the process is repeated." (Emphasis added)

Effectively, Giroux et al. prevents the customer from simultaneously having possession of more than a single decryption key. If the method taught by Giroux et al. were applied to video content, the customer would not receive the decryption key to decrypt the next segment of encrypted video content until after the previous segment was decrypted, displayed and deleted along with the previous decryption key. This would effectively prevent uninterrupted viewing of video content, as there would be some delay when the Application utility 230 "clears the buffers to destroy the decrypted version of the section" and then has to repeat the decryption key request to receive the next decryption key.

**Ginter et al.**

Ginter et al. describes an integrated, modular array of administrative and support services for electronic commerce and electronic rights and transaction management in an effort to provide a secure foundation for conducting financial management, rights management, certificate authority, rules clearing, usage clearing, secure directory services, and other transaction related capabilities functioning over an electronic network such as the Internet and/or over organization internal Intranets.

Ginter et al. describes a "super distribution" implementation in which protected digital content is distributed from "upstream" customers to "downstream" customers, wherein the protected digital content includes payment/access controls that must be satisfied by the customer in order to access the digital content. The Examiner has specifically pointed to Figure 28 of Ginter et al., which illustrates an example of "super distribution".

**Granger et al.**

Granger et al. describes three methods for protecting software applications from unauthorized distribution and use. The first method involves using values generated by a conventional ESD (Electronic Security Device) to encrypt and/or decrypt user data (such as a file) that is generated and used by the application. In one embodiment, the user data is encrypted using values returned by the ESD, and the user data is later decrypted using like values returned by a software-implemented ESD simulator. The second and third methods involve the use of special development tools in an effort to make the task of analyzing the application's copy protection code (such as the code used to encrypt and/or decrypt user data) more difficult. Specifically, the second method involves using pseudocode to implement some or all of the application's copy protection functions. The pseudocode for a given function is generated from actual code using a special development tool, and is then imbedded within the application together with a corresponding pseudocode interpreter. The interpreter fetches, decrypts and executes the pseudocode when the function is called. The third method involves the use of an obfuscation tool to convert the code for selected copy-protection functions into long, inefficient sequences of machine code.

The Examiner has specifically pointed to Figures 1A and 1B of Granger et al. In Figures 1A/1B of Granger et al., a seed value is provided to an ESD/ESD Simulator to generate an encryption/decryption key to encrypt/decrypt user data. It is important to note that the ESD/ESD simulator creates the encryption/decryption key based only on the seed value. The encryption/decryption key is not based in any way on user-specific information.

**Watanabe**

Watanabe describes a digital contents generating apparatus connected with a communication network that includes an electronic watermark-data embedding unit for embedding electronic watermark data in digital contents, an encryption unit for encrypting the digital contents embedded with electronic watermark data by an encryption key received from an encryption-key generating unit, and a decryption-key generating unit for generating a decryption key. A digital contents reproducing apparatus connected with the communication network includes an electronic watermark data extraction unit for extracting electronic watermark data from encrypted digital contents embedded with electronic watermark data, and a decryption unit for decrypting the encrypted digital contents using a predetermined decryption key.

In one of the examples described in Watanabe, the encryption-key generating unit generates an encryption key based in part on the IP address of a user to whom the digital content is to be transmitted (See column 5, lines 17 to 35).

*Ascertaining The Differences Between The Prior Art And The Claims At Issue*

Claim 1

Independent claim 1 recites:

> 1. A method of delivering data content from a data content provider to a customer processing platform and controlling use of the data content at the customer processing platform, comprising:
>
> encrypting each of a plurality of sections of the data content using a respective one of a plurality of encryption keys to produce a corresponding plurality of encrypted sections;
>
> delivering the plurality of encrypted sections to the customer processing platform; and
>
> delivering to the customer processing platform a plurality of decryption keys corresponding to the plurality of encryption keys, wherein the decryption keys are delivered in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time, wherein delivering the plurality of decryption keys comprises:
>
> delivering to the customer processing platform a current key of the plurality of decryption keys;
>
> delivering to the customer processing platform a next key of the plurality of decryption keys; and
>
> causing the current key to be destroyed at the customer processing platform only after at least the next key of the plurality of decryption keys has been received. (Amendments underlined)

**Peterka et al.**

As noted above, the Examiner concedes that Peterka et al. does not disclose "delivering to the customer processing platform a plurality of decryption keys corresponding to the plurality of encryption keys, wherein the decryption keys are delivered in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time".

While Peterka et al. may teach that "two PSK are distributed at a given time" and "that a client has possession of program segment key and the next key ... as well as content key 0, 1, 2, 3, 4, ...", it is respectfully submitted that simply making available only a subset of the PSKs at any given time does **not** guarantee that the client only has simultaneous possession of at most a subset of the PSKs. Accordingly, there is no suggestion in Peterka et al. that if all of the decryption keys have been delivered to the client, the client only has simultaneous possession of at most a subset of the plurality of decryption keys. In fact, the Examiner's own admission that the "client has possession of program segment key and the next key ... **as well as the content keys 0, 1, 2, 3, 4, ...**" (emphasis added), illustrates that according to Peterka et al., the client has simultaneous possession of **all** of the content keys once all of the content keys have been received by the client. In contrast, embodiments of the present invention prevent a client from simultaneously having all of the encrypted content and all of the decryption keys necessary to decrypt the encrypted content. Peterka et al. does not provide this same anti-piracy functionality.

**Feig et al.**

As noted above, the portions of Feig et al. that the Examiner has referred to in rejecting the claims, and Feig et al. as a whole, fails to teach or even suggest "delivering to the customer processing platform a plurality of decryption keys corresponding to the plurality of encryption keys, wherein the decryption keys are delivered in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time". Feig et al. merely discloses the sequential streaming of token keys to a client receiver and the decryption of encrypted content using the streamed token keys.

In the teachings of both Peterka et al. and Feig et al. the customer **retains possession** of the decryption keys and the decrypted content, i.e., by the end of a program (end of decryption of last encrypted program segment), the customer has all of the decrypted content and the full set of decryption keys, thereby allowing unrestricted access/use of the decrypted content. The customer could then potentially copy and distribute the decrypted content and/or the decryption keys and encrypted content. Accordingly, the teachings of Peterka et al. and Feig et al., both alone and in combination, fail to provide the anti-piracy protection provided by unamended independent claim 1.

In view of the foregoing, Applicant submits that the Examiner has not properly determined the differences between unamended independent claim 1 and the prior art. Therefore, the findings of fact as articulated by the Examiner in rejecting unamended independent claim 1 are improper.

Furthermore, as indicated above, amended independent claim 1 recites *inter alia*:

> "wherein delivering the plurality of decryption keys comprises:
>
> delivering to the customer processing platform a current key of the plurality of decryption keys;
>
> delivering to the customer processing platform a next key of the plurality of decryption keys; and
>
> causing the current key to be destroyed at the customer processing platform only after at least the next key of the plurality of decryption keys has been received."

Clearly, Peterka et al. and Feig et al. fail to teach or even suggest such a feature, as neither reference even contemplates preventing the customer from retaining all of the decryption keys once they have been delivered to the customer, as established above.

Former dependent claim 3 recited the delivery of a current key and a next key and the destroying of the current key, but did not explicitly recite when the current key was destroyed in relation to the receiving of the next key. Former dependent claim 3 was rejected under 35 U.S.C. 103(a) as being unpatentable over Peterka et al. in view of Feig et al. and further in view of Giroux et al.

**Giroux et al.**

As noted above, Giroux et al. teaches that a next decryption key is not delivered to a customer until the previous decryption key has been deleted and the decrypted content of the previous encrypted segment has been displayed and deleted. That is, the customer only ever has possession of a single decryption key at a time.

In contrast, amended independent claim 1 recites delivery of a current decryption key and the next decryption key to a customer processing platform and the destroying of the current key only after at least the next key has been received. This feature of amended independent claim 1 allows the buffering of encrypted sections of data content and a subset of the plurality of decryption keys to decrypt the encrypted sections, so that decryption and playback of the data content can be seemless and uninterrupted. It should be noted that amended independent claim 1 covers embodiments in which the first decryption key of the plurality of decryption keys is destroyed at any time after at least the second decryption key has been received. For example, amended independent claim 1 covers the following scenarios:

> a) the customer processing platform receives the first decryption key and the second decryption key and deletes the first decryption key when decryption of the first encrypted section is completed and decryption of the second encrypted section has begun. (e.g. the first decryption key is deleted before the third decryption key is received, such that the customer processing platform only ever has simultaneous possession of two decryption keys); and
>
> b) the customer processing platform receives a current decryption key and any subset of the remaining decryption keys and destroys the current decryption key before all of the decryption keys are received (e.g., for a set of N decryption keys, the customer processing platform may receive decryption keys 1 to X, where X < N, such that after receiving the second decryption key and decrypting the first encrypted section the first decryption key may be deleted at any time before the last decryption key N is received).

By having at least two decryption keys of the plurality of decryption keys, as recited in amended independent claim 1, the customer processing platform is able to process the encrypted data content in a manner that allows for uninterrupted playback of, for example, encrypted video content, while delivering the decryption keys in a manner such that the customer processing platform on has simultaneous possession of at most a subset of the plurality of decryption keys controls the usage of the encrypted data content, as the customer processing platform never has a complete set of decryption keys, thereby preventing unauthorized decryption and playback of the encrypted data content. No combination of Peterka et al., Feig et al. and Giroux et al. provides the foregoing features of amended independent claim 1.

In view of the foregoing, Applicant respectfully submits that amended independent claim 1 is both novel and inventive over the cited references, as no combination of the cited references teaches all of the novel and inventive features of amended independent claim 1.

Independent claims 16, 34, 35, 38 and 40

Unamended independent claims 16, 34, 35, 38 and 40 were rejected under 35 U.S.C. 103(a) as being unpatentable over Peterka et al. in combination with Feig et al. (claims 35, 38 and 40), Peterka et al. in combination with Feig et al. and Giroux et al. (claim 34), or Feig et al. in combination with Giroux et al. (claim 16). Amended independent claims 16, 34, 35, 38 and 40 include amended features similar to those of amended independent claim 1, i.e., possession of a current decryption key and the next decryption key and deleting/destroying the current decryption key only after at least the next decryption key has been received. Accordingly, Applicant respectfully submits that amended independent claims 16, 34, 35, 38 and 40 are novel and inventive over Peterka et al., Feig et al. and Giroux et al., both alone and in combination, for at least the reasons stated above with respect to amended independent claim 1.

Dependent claims 7-10, 13, 15, 17, 18, 21, 36, 41 and 42

Dependent claims 7-10, 13, 15, 36, 41 and 42 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Peterka et al. in view of Feig et al.

Dependent claims 17, 18 and 21 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Feig et al. in view of Giroux et al.

By virtue of their claim dependencies on one of the amended independent claims, Applicant respectfully submits that dependent claims 7-10, 13, 15, 17, 18, 21, 36, 41 and 42 are novel and inventive over Peterka et al. and Feig et al. for at least the same reasons.

Furthermore, Applicant respectfully submits that dependent claims 7 and 10 recite features that further patentably distinguish over Peterka et al. and Feig et al., as noted below.

Claim 7 recites in part:

> "billing a customer for delivery of the encrypted sections, and then billing the customer each time the data content is used at the customer processing platform".

The Examiner has pointed to Figures 8 and 9 and paragraph [0111] of Peterka et al. in support of the rejection of claim 7. Figures 8 and 9 of Peterka et al. illustrate encrypted data content distribution methods that include: receiving a request for a cryptographic key from a client; logging the request for the key; logging a segment of the program content for which the key can be used; distributing one or more decryption keys; **distributing program content for decryption by the client utilizing the key; and billing the client based upon log entry(ies).** Therefore, according to Figures 8 and 9 of Peterka et al., and Peterka et al. as a whole, a client must request the cryptographic key **and download the program content again** each time the client wishes to use the data content. According to the teachings of Peterka et al., the client is only billed once the client has re-downloaded the key and the program content, which is completely different than "billing a customer for delivery of the encrypted sections, and then billing the customer each time the data content is used at the customer processing platform", as recited in claim 7.

Claim 10 recites:

> 10. The method of claim 1, further comprising:
>
> generating each of the plurality of <u>encryption keys</u> using an identifier associated with the customer processing platform, to thereby generate a plurality of customer processing platform-specific keys. (Emphasis added)

In rejecting claim 10, the Examiner has pointed to Figure 21 and paragraphs [0146], [0114] and [0124] of Peterka et al. However, these portions of Peterka et al., and Peterka et al. as a whole, merely describe the use of a key that is unique to a client to encrypt content decryption keys before they are sent to the client. The client then decrypts the encrypted content decryption keys using their unique key and uses the decrypted content decryption key to decrypt encrypted content. It is important to note that the encrypted content was not encrypted with customer-specific encryption keys that were generated using an identifier associated with the customer processing platform, rather the encrypted content was encrypted with a generic set of encryption keys, and when the client requests the decryption keys, the key server uses the client's unique key to encrypt the decryption keys, thus creating customer-specific decryption keys. This distinction is important because the encrypted content delivered according to Peterka et al. is generic, i.e., there is nothing customer-specific about the encrypted content, whereas according to claim 10, the encrypted content is encrypted with encryption keys that are generated using an identifier associated with the customer processing platform. According to the teachings of Peterka et al., the encrypted content keys are decrypted with the higher level key, i.e. the unique key (UK), and the content keys are then used to decrypt the corresponding program segments. Once the content key is decrypted with the higher level key, it is completely untraceable, as any customer specific information has been stripped during the decryption of the content key. In contrast, the method according to claim 22 provides for traceability of the decryption key and the encrypted data content, because the sections of data content are encrypted with customer processing platform-specific keys.

It should also be noted that the "identifier" described in Figure 21 and paragraph [0146] of Peterka et al., which the Examiner has relied upon in rejecting claim 10, is not "an identifier associated with the customer processing platform" rather it is a program content identifier that the customer sends to a caching server to identify the specific program content that the user of the client computer desires to obtain. Clearly using an identifier that identifies specific program content to generate encryption keys to encrypt the specific program content would not result in customer-specific encryption keys.

Dependent claims 11 and 12

Dependent claims 11 and 12 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Peterka et al. in view of Feig et al. and further in view of Granger et al. By virtue of their claim dependencies on amended independent claim 1, Applicant respectfully submits that dependent claims 11 and 12 are novel and inventive over Peterka et al., Feig et al. and Granger et al. for at least the same reasons.

Dependent claims 11 and 12 are dependent on claim 10, and therefore distinguish over Peterka et al. and Feig et al. for at least the same reasons as stated above with respect to claim 10. Granger et al. similarly fails to teach or even suggest generating the encryption keys using an identifier associated with a customer processing platform, as recited in claim 10. Accordingly, claim 10, and claims 11 and 12, by virtue of at least their claim dependencies on claim 10, are also novel and inventive over Granger et al.

Furthermore, Applicant respectfully submits that dependent claim 11 recites features that patentably distinguish over Peterka et al., Feig et al. and Granger et al., as noted below.

Claim 11 recites:

> 11. The method of claim 10, wherein generating comprises generating each of the plurality of customer processing platform-specific keys <u>using the identifier and a respective key generation seed value</u>.

As noted above with respect to claim 10, Peterka et al. fails to teach or even suggest generating encryption keys using an identifier associated with the customer processing platform, rather Peterka et al. describes encrypting decryption keys (content keys (CK)) with a higher level key that is unique to a particular customer (unique key (UK)) before delivering the encrypted decryption keys to the customer. Accordingly, Peterka et al. clearly fails to teach or even suggest generating each of the plurality of customer processing platform-specific keys <u>using the identifier and a respective key generation seed value</u>, as recited in claim 11. In rejecting claims 11 and 12, the Examiner has relied on the teaching in Granger et al. of using seed values and an ESD to generate encryption keys. However, Granger et al. fails to teach or even suggest using a respective key generation seed value <u>and</u> an identifier associated with a customer processing platform to generate customer-processing specific keys.

<u>Dependent claims 4-6 and 39</u>

Dependent claims 4-6 and 39 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Peterka et al. in view of Feig et al. and further in view of Giroux et al. By virtue of their claim dependencies on one of the amended independent claims, Applicant respectfully submits that dependent claims 4-6 and 39 are novel and inventive over Peterka et al., Feig et al. and Giroux et al. for at least the same reasons.

Furthermore, Applicant respectfully submits that amended dependent claim 39 recites features that further patentably distinguish over Peterka et al., Feig et al. and Giroux et al., as noted below.

Amended claim 39 recites:

> 39. The system of claim 38, wherein the customer processing platform comprises:
>
> means for requesting the data content to be delivered to the customer processing platform via a peer-to-peer network connection;
>
> means for receiving the plurality of encrypted sections via the peer-to-peer network connection;
>
> means for receiving, for each encrypted section, the decryption key in respect of the encrypted section over an encrypted decryption key delivery channel; and
>
> means for decrypting and playing back the encrypted section using the decryption key~~; and~~, wherein
>
> the means for destroying the current decryption key comprises means for destroying the current decryption key~~,~~ after completing playback of the current encrypted section and beginning playback of the next encrypted section.

Effectively, amended claim 39 recites delivery of encrypted data content via a peer-to-peer network, while the decryption keys are retrieved over a secure encrypted decryption key delivery channel. The encrypted content can be freely shared between customers, only requiring interaction with the data content to securely deliver the decryption keys when the client wishes to access the encrypted content. Peterka et al., Feig et al., and Giroux et al. fail to teach or even suggest peer-to-peer delivery of encrypted content and separate secure delivery of encrypted decryption keys over an encrypted decryption key delivery channel.

Furthermore, amended claim 39 recites that the current decryption key is destroyed after completing playback of the current encrypted section and beginning playback of the next encrypted section. In contrast, Giroux et al. requires that a current decryption key be deleted immediately upon completion of decryption of the current encrypted segment, and only allows delivery of the next decryption key once the current decrypted content has been displayed and deleted (See paragraph [0051]).

Dependent claims 14, 20 and 43

Dependent claims 14 and 43 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Peterka et al. in view of Feig et al. and further in view of Ginter et al.

Dependent claim 20 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Feig et al. in view of Giroux et al. and further in view of Ginter et al.

The Examiner has relied on Ginter et al. for allegedly teaching the delivery of encrypted content between customer processing platforms. Ginter et al. fails to teach or even suggest the novel and inventive features of the amended independent claims that clearly distinguish over Peterka et al., Feig et al. and Giroux et al., as established above. Accordingly Applicant respectfully submits that the amended independent claims are novel and inventive over Peterka et al., Feig et al., Giroux et al. and Ginter et al.

By virtue of their claim dependencies on one of the amended independent claims, Applicant respectfully submits that dependent claims 14, 20 and 43 are novel and inventive over Peterka et al., Feig et al., Giroux et al. and Ginter et al. for at least the same reasons.

Furthermore, Applicant respectfully submits that amended dependent claims 14 and 20 recite features that further patentably distinguish over Peterka et al., Feig et al., Giroux et al. and Ginter et al., as noted below.

Amended claims 14 and 20 recite in part:

> "the plurality of decryption keys are encrypted using a <u>public cryptographic key corresponding to a private cryptographic key</u> known only to the customer processing platform." (emphasis added)

As noted above, Peterka et al. describes the encryption of decryption keys (content keys (CK)) with a higher level key that is unique to a particular customer (unique key (UK)). Peterka et al. also describes the encryption of decryption keys (content keys (CK)) with a higher level, such as a Program Key (PK), Free Preview Key (FPK) or a Group Key (GK), which are not unique to a particular customer (See Paragraph [0124]). However, Peterka et al. fails to teach or even suggest encrypting a plurality of decryption keys using a <u>public cryptographic key corresponding to a private cryptographic key</u> known only to the customer processing platform. While the Unique Key (UK) described by Peterka et al. is unique to a particular customer, i.e., known only to the customer processing platform, Peterka et al. does not teach that a public cryptographic key, corresponding to the Unique Key is used to encrypt content keys (CK).

None of the other cited references even suggest the encryption of decryption keys, and therefore clearly do not teach or even suggest the foregoing feature of amended claims 14 and 20.

<u>Dependent claim 19</u>

Dependent claim 19 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Feig et al. in view of Giroux et al. and further in view of Granger et al. By virtue of its claim dependency on amended independent claim 16, Applicant respectfully submits that dependent claim 19 is novel and inventive over Feig et al., Giroux et al. and Granger et al. for at least the same reasons.

<u>Dependent claims 22 and 23</u>

Dependent claims 22 and 23 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Feig et al. in view of Giroux et al. and further in view of Watanabe.

The Examiner has relied on Watanabe for teaching the generation of encryption keys based on an IP address of the customer processing platform. However, Watanabe is entirely silent with respect to "destroying the decryption key only after completing playback of the encrypted section and beginning playback of the next encrypted section", as recited in amended independent claim 16, from which claims 22 and 23 depend. Accordingly, in addition to being novel and inventive over Peterka et al., Feig et al. and Giroux et al., amended independent claim 16, and the other amended independent claims, are also novel and inventive over Watanabe.

By virtue of their claim dependencies on amended independent claim 16, Applicant respectfully submits that dependent claims 22 and 23 are novel and inventive over the cited references for at least the same reasons.

New dependent claims 44, 45, 47, 48, 49, 50 and 52

Applicant respectfully submits that new dependent claims 44, 45, 47, 48, 49, 50 and 52 are novel and inventive over the cited references.

Similar to amended dependent claim 39, new dependent claims 44, 45, 47, 48, 49, 50 and 52 recite destroying/deleting a current decryption key only after processing of the next encrypted section with the next decryption key has begun. As noted above with respect to claim 39, Giroux et al. requires that a current decryption key be deleted immediately upon completion of decryption of the current encrypted segment, and only allows delivery of the next decryption key once the current decrypted content has been displayed and deleted (See paragraph [0051]). This teaches away from the claimed invention, and cannot be found to render the claimed invention obvious.

New dependent claims 46, 51 and 53

Applicant respectfully submits that new dependent claims 46, 51 and 53 are novel and inventive over the cited references.

Similar to amended dependent claim 39, new dependent claims 44, 45, 47, 48, 49, 50 and 52 recite delivery of encrypted data content via a peer-to-peer network, while the decryption keys are retrieved over a secure encrypted decryption key delivery channel. Applicant respectfully submits that such a feature is novel and inventive for at least the reasons stated above with respect to claim 39.

*Conclusion*

In view of the foregoing, Applicant respectfully submits that claims 1, 4-23, 34-36 and 38-53 are both novel and inventive over the cited references, both alone and in combination, and requests that the Examiner withdraw the rejections under 35 U.S.C. 103(a).

Early favorable consideration of this application is earnestly solicited. In the event that the Examiner has concerns regarding the present response the Examiner is encouraged to contact the undersigned at the telephone number listed below.

Respectfully submitted,

VINCENT SO

By

Allan Brett
Reg. No. 40,476
Tel.: (613) 232-2486 ext. 323

Date: April 7, 2008

RAB:JFS:mhg